U.S. FISH AND WILDLIFE SERVICE TRANSMITTAL SHEET

PART	SUBJECT	RELEASE NO.
270 FW 2	IT Program Management Automated Information Systems Capital Planning and Management	439
FOR FURTHER INFORMATION CONTACT Division of Information Resources and Technology Management		DATE February 17, 2004

EXPLANATION OF MATERIAL TRANSMITTED:

This revised chapter adopts better nomenclature to clarify policies, aligns terminology with other IT areas such as security, and reflects changes in the IT capital planning process.

Acting DIRECTOR

FILING INSTRUCTIONS:

Remove:	Insert:
270 FW 2, 09/30/02, FWM 406	270 FW 2, 02/17/04, FWM 439

Chapter 2 Automated Information Systems Capital Planning and Management 270 FW 2

2.1 What is the purpose of this chapter? This chapter defines Fish and Wildlife Service (Service) policies for planning and managing investments in information technology (IT) and automated information systems (AIS). The goal is to ensure that Service investments in IT and AIS are made, managed, and documented on a sound business basis, reflect strategic goals of the Service, and comply with applicable Service, Departmental, and Federal policies. The aim is to improve the productivity, efficiency, and effectiveness of Service programs by ensuring that investments in IT and AIS are linked to mission and budget and are managed in accordance with validated business processes.

2.2 To whom does this chapter apply? This chapter applies to Regions, California/Nevada Operations Office (CNO), and all Service offices that initiate and fund IT and AIS, or deploy IT in support of Department of the Interior mandated AIS.

2.3 How does this chapter relate to other Service policies? This chapter deals with the general requirements for initiating and funding an AIS to become part of the Service's IT investment portfolio and for managing its life cycle. 270 FW 1 states policy on IT architecture with which Service systems must conform. 270 FW 4 articulates the requirements to integrate periodic reviews into the life cycle. 270 FW 7 focuses on specific IT security requirements that are a critical part of a system's life cycle.

2.4 What is our authority for taking this action? There are several Federal and Departmental laws and guidelines that mandate the establishment of an IT capital planning program in the Service. The most important ones are:

A. Government Performance and Results Act (GPRA) of 1993, Pub. L.103-62**.**

B. Information Technology Management Reform Act of 1996 (ITMRA or the Clinger-Cohen Act)**.**

C. OMB Circular A-11, Parts 2, 6, and 7.

D. OMB Circular A-130.

2.5 What is the Service's policy on IT planning and management?

A. Every Service major application (MA) and general support system (GSS), as defined in paragraph 2.7, must be properly documented by a project charter and tracked in the Service's Catalog of Automated Information Systems (CAIS) (see paragraph 2.8).

B. Annual multi-year funding information for every MA and GSS must be tracked in the Service's IT Investment Portfolio (OMB Circular A-11, Exhibit 53). Information must include the annual costs of development, modernization, enhancement, maintenance, and other related activities. This requirement also pertains to Service deployment of IT in support of Departmentally mandated AIS.

C. Major IT investments, as defined in paragraph 2.7, must be documented and kept up to date by a Capital Asset Plan and Business Case in the format of OMB Circular A-11, Exhibit 300. All other MA and GSS must be documented and kept up to date by a Project Profile in the format of Exhibit 300-1 ("300 lite").

D. Project documentation for MA and GSS described in 2.5A and 2.5C must be circulated to the Chief Technology Officer (CTO) Council for review, and the Service CTO will review and approve projects (see paragraph 2.6).

E. All MA and GSS will follow a documented life cycle methodology (see paragraph 2.10).

2.6 Who is responsible for implementing the provisions of this chapter?

A. Regional Directors; Manager, CNO; Chief, Law Enforcement; and Assistant Directors are responsible for ensuring that their staffs implement these policies and procedures.

B. The **Service IT Capital Planner** is responsible for:

(1) Gathering and maintaining information for the Service's IT investment portfolio and the CAIS to reflect new and updated information on MA and GSS on an annual basis.

(2) Reviewing and circulating project charters to Regional/CNO and Program CTO's for review and comments, incorporating comments, and preparing the project package for approval by the Service CTO.

(3) Providing updates to the Department's IT Investment Portfolio (reported in OMB Circular A-11, Exhibit 53).

(4) Coordinating the submission and updates of Business Cases (Exhibit 300) and Project Profiles (Exhibit 300-1) for the Service's major applications and GSS to the Department.

C. The **Service Chief Technology Officer** is responsible for:

(1) Designating Service AIS as major applications and GSS.

(2) Designating whether or not an MA or GSS is a major investment.

(3) Advising AIS owners on compliance with Service IT standards and architecture and opportunities for data integration and sharing.

(4) Elevating to the CTO Council for resolution issues that raise questions about proceeding with development.

D. AIS Owners and Project Managers are responsible for:

(1) Ensuring that the planning, budgeting, staffing, acquisition, development, implementation, and maintenance of AIS under their management are in compliance with OMB Circular A-11, Section 300; OMB Circular A-130; 270 FW 7; 270 FW 1; and 270 FW 4 .

(2) Ensuring that project charters are prepared (see paragraph 2.8) and kept up to date for all of their systems.

(3) Ensuring that Business Cases in the format of OMB Circular A-11, Exhibit 300 are prepared for their major IT investments and kept up to date.

(4) Ensuring that Project Profiles in the format of Exhibit 300-1 ("300 lite") are prepared for their non-major IT investments and kept up to date.

(5) Ensuring that project charters for new MA and GSS and their Capital Asset Plans or Project profiles are submitted to the Service's IT capital planner for review (see paragraph 2.9).

(6) Following a life cycle methodology for their MA and GSS (see paragraph 2.10).

(7) Providing (generally on an annual basis) funding information and updated copies of Capital Asset Plans and/or Project Profiles to the Service IT capital planner to update the Service's IT investment portfolio. Documenting whether funding sources of increased AIS expenditures are from existing base budgets or are reflected in new budget requests.

(8) Ensuring that their MA and GSS are accurately described in the CAIS by providing the Service CTO with an updated description annually.

(9) Ensuring that their AIS incorporate the IT security provisions described in 270 FW 7, including the requirement that MA and GSS have system security plans and are properly certified and accredited.

E. Regional/CNO and Program CTO's are responsible for:

(1) Commenting on project charters circulated for review by the Service CTO.

(2) Supporting the implementation of chartered AIS within their Region/CNO or Program .

F. The **CTO Council** will:

(1) Review Capital Asset Plans prior to submission to the Department.

(2) Resolve issues that raise questions about proceeding with development, such as the classification of a system as a major IT investment, or compliance with Service IT standards and architecture.

(3) Review and approve major IT investments, other than Departmentally mandated systems, on the basis that the investment serves Service goals in a cost effective manner.

G. User Acceptance Teams are responsible for:

(1) Defining and developing functional requirements.

(2) Participating in the evaluation and testing of the system.

(3) Recommending to the AIS owner whether or not to accept the system.

2.7 What special terms do I need to know?

A. Automated Information System (AIS). A discrete set of information and IT organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. AIS's include, but are not restricted to, local and wide area networks, telecommunications systems, electronic mail systems, geographic information system (GIS) projects, data creation projects, databases, and radio projects. See the

definitions of "major application" and "general support system" for two important kinds of AIS.

B. AIS Life Cycle. The period of time from the conception of an AIS through implementation, operations, and maintenance to retirement.

C. AIS Life Cycle Costs. The total cost expended for an AIS over all stages of its life cycle, including equipment, salaries, contracts, training, etc.

D. AIS Project Manager. The person appointed by the AIS owner who is responsible for direct management of all aspects of the system's development and life cycle.

E. AIS Owner. The senior management official having overall functional responsibility for the program or activity in which a specific AIS is conceived, planned, funded, developed, acquired, operated and maintained. The AIS owner is at least one supervisory level above those who are responsible for system development.

F. Catalog of Automated Information Systems (CAIS). A database describing AIS owned by the Service. The CAIS is available to Service personnel to enable them to learn what systems exist in the Service and to avoid duplicating systems and data.

G. Chief Technology Officers (CTO) Council. The group that will fulfill oversight requirements of the Clinger-Cohen Act and OMB Circular A-11 and which is comprised of the Service CTO, Regional/CNO CTO's, and Program CTO's, as well as a rotating member from the Deputies Group (Deputy Assistant Directors and Deputy Regional/CNO Directors) and a rotating member who is an Assistant Regional Director–Budget and Administration. The CTO Council reviews and advises the Directorate on proposed AIS, and makes budgetary and deployment recommendations to the AIS owner and the Director based upon overall Service priorities and requirements.

H. Financial System. An AIS used for any of the following:

(1) Collecting, processing, maintaining, transmitting, and reporting data about financial events.

(2) Supporting financial planning or budgeting activities.

(3) Accumulating and reporting cost information.

(4) Supporting the preparation of financial statements.

I. General Support System (GSS). Term from OMB Circular A-130, Appendix III, meaning an interconnected set of information resources under the same direct management control that shares common functionality and normally includes hardware, software, information, data, applications, communications, and people. Examples are local and wide area networks, telecommunications systems, and electronic mail systems.

J. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Typically, IT includes hardware and software pertaining to computers, telecommunications, networks, and radio equipment.

K. IT Capital Asset Plan. A formal plan in the format of OMB Circular A-11, Exhibit 300, that documents the information that will be used to design a major IT investment, to assess the benefits and risks of alternative solutions, and to establish realistic cost, schedule and performance goals.

L. IT Investment Portfolio . An inventory of existing MA and GSS that captures annual costs of development, modernization, enhancement and maintenance. The Service reports its IT Investment Portfolio to the Department in Exhibit 53 of OMB Circular A-11.

M. IT Project Profile . A formal description of an IT Project in the form of Exhibit 300-1 ("300 lite") used by the Department to document non-major IT investments.

N. Major Application (MA) . Term from OMB Circular A-130, Appendix III, meaning an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Do not confuse this term with the term "major IT investment" defined below to designate certain levels of capital investment for a system. Applications that meet any of the following criteria will be considered by the Service to be MA:

(1) Runs over a Service or Departmental network.

(2) Is shared by more than one Region/CNO or Program.

(3) Requires user authentication for access.

(4) Is a financial system .

(5) Access to data could benefit someone financially.

(6) Is a personnel/payroll system.

(7) Contains privacy data.

(8) Contains Indian trust data.

(9) Total life cycle costs exceed $1M.

(10) Interfaces with other Federal, State, or local governments.

(11) Supports critical Federal activities like law enforcement or fire management.

O. Major IT Investment . As defined by OMB Circular A-11, an AIS that requires special management attention because of its (1) importance to a Service mission; (2) high development, operating or maintenance costs; or (3) high risk systems that have a significant role in the administration of Service programs, finances, property, or other resources. A system will meet criterion (2) if its total life cycle costs (development, operating, and maintenance) exceed $35M (or annual cost of $500,000 for financial systems). Do not confuse this term with "major application" defined above.

P. Program Chief Technnology Officer (Program CTO). A person designated by a Program or office to coordinate IT issues between that Program or office and the Division of ITM.

Q. Regional/CNO Chief Technology Officer (Regional CTO). The person designated by each Region/CNO to coordinate IT issues between that Region/CNO and the Division of ITM.

R. Service Chief Technology Officer (Service CTO). The official who is responsible for coordinating IT issues on a Servicewide basis and for ensuring that information resources support the Service's strategic missions. The Service CTO is the Chief of the Division of Information Resources and Technology Management - Washington Office.

S. Service Information Technology Capital Planner. The person designated by the Service CTO to be responsible for IT capital planning and investment control coordination in the Service, as required by OMB Circular A-11 and the Department.

T. User Acceptance Team. Team comprised of representatives from the user community that have the appropriate expertise to define and assess functional requirements for an AIS.

2.8 What is a project charter? A project charter must be prepared for all MA and GSS using FWS Form 3-2230 (Project Charter). Charters are also recommended for other systems. The charter ensures that the AIS owner has a thorough understanding of the system before investing resources in development. The project charter is also used to communicate plans for the system within the Service IT community to avoid duplication, to facilitate partnerships, and to ensure a thorough understanding within the IT community of the proposed system's impact on existing Servicewide and Regional network infrastructures. A charter provides the raw material for creating the initial description of the system in the CAIS. This document is also a vehicle for the Service Chief Technical Officer to communicate any concerns or issues concerning the system to the owner. Finally, it is the vehicle whereby the Service CTO will certify the compliance of the system with Service and Departmental IT standards and architecture as well as recommend whether the system should be considered a major IT investment. Project charters are not static documents and need to be updated as systems change.

2.9 What is the process for reviewing project charters?

A. The owner of an MA or GSS will submit a project charter to the Service's IT capital planner in the Division of Information Technology Management. If it is a major IT investment as defined in paragraph 2.7, the owner must attach a Capital Asset Plan in the format of OMB Circular A11, Exhibit 300 and any pertinent supporting documentation, such as Federal Register notices, Privacy Act notices, supporting laws, etc. All others must have a Project Profile in the format of Exhibit 300-1 ("300 lite") attached.

B. The Service's IT capital planner will circulate the charter and accompanying documentation by electronic mail to the Regional/CNO and Program CTO's for review and comments for a period of 10 working days. Major IT investments may require additional time for review, but the period will not exceed 30 calendar days.

C. The Service's IT capital planner will consolidate comments on the charter and submit it to the Service CTO for approval.

D. The Service CTO will recommend whether to proceed with the project as described, to proceed with recommended changes, or to terminate the project.

E. After CTO signature, the IT capital planner will return the charter with comments and recommendations to the system owner and enter project information into the CAIS.

F. If the Service CTO has an unresolved disagreement with the system owner on an issue that raises a question about proceeding with development, the system owner may document the disagreement and ask the CTO to submit the charter to the CTO Council for resolution.

2.10 What is the Service's Life Cycle Management policy? System owners should use an evolutionary methodology that reflects current information technologies such as the Internet, that can accommodate changes in information needs and technologies during the development and operation of a system, and that supports rapid prototyping. The following sequence describes the minimal requirements for development of any MA or GSS. All stages must be well documented.

A. Identify the problem or need, based on plans and priorities of a Service office or Program.

B. Review the AIS in the CAIS before beginning development of a new system in order to avoid duplicating an existing system or a system under development.

C. Appoint a project manager and a user acceptance team. The project manager should be trained in Systems Development Life Cycle Methodology. In order to achieve a broad range of feedback, the user acceptance team should be comprised of technical staff, end users, program personnel, and management. General SDLC guidance for IT systems can be found in the Service SDLC Guidebook.

D. Clearly define what results are required to satisfy the need, and what resources (staff/funding) are available.

E. Create a project charter for the system (and a Capital Asset Plan for major IT investments) using FWS Form 3-2230 (see paragraph 2.8) and submit it for review per paragraph 2.9. Revise the charter if necessary. Documentation should include, where appropriate, items that address the following:

(1) Privacy and records management to ensure that the system has effective security controls and authentication tools to protect privacy and that the processing of personal information is in compliance with the Privacy Act of 1974 and other relevant Governmentwide and agency policies.

(2) The Government Paperwork Elimination Act (GPEA) to ensure considered feasibility of an option to conduct those transactions electronically and to maintain electronic records of the transactions.

(3) Section 508 of the Rehabilitation Act Amendments of 1998, which require that information technology be accessible to disabled employees as much as practicable.

F. Define performance measures that allow comparison of actual performance to expected results.

G. Define control processes that will be used to assure that project budget, schedule, and quality are met.

H. Evaluate alternative solutions and select an appropriate one.

I. Establish a project plan by documenting the schedule and strategies for design, development, acquisition, testing, training, deployment, and maintenance. Include all relevant phases and milestones, including hardware and software to be procured, and applications to be developed. For each phase/milestone, describe the criteria of success that will be used to evaluate progress and to justify funding the next phase/milestone. Determine costs of each phase. Plan and budget for IT security (see 270 FW 7).

J. Build and acquire a system that will produce the results described in the project charter and other project documentation.

K. Develop IT security documentation as required by 270 FW 7 .

L. Test the system and its security features to make sure it works, based on feedback from the user acceptance team.

M. Formally certify and accredit the system in accordance with Service and Departmental requirements .

N. Implement the system and train employees to use it properly.

O. Review the system and its documentation periodically to ensure that they are kept current, measure actual performance against performance goals, and make changes as necessary based on feedback from the user acceptance team. Provide updates to the Service CTO to reflect changes for the CAIS.

P. Perform periodic independent reviews or audits of IT security controls in the system security plan (see 270 FW 7) at least every 3 years or when significant changes are made to the system. See 270 FW 4 and NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," for further information.